



PRIVACY PROGRAM



Transformation
through Partnerships

Department of Energy
2012 IMC Conference

Jerry Hanley
Chief Privacy Officer



Office of the Chief
Information Officer

Privacy Office

Privacy Order

SSN Plan

New PIA Process

FISMA Reporting

Future

- The Privacy Office: Objectives
- Privacy Order DOE Order 206.1, *Department of Energy Privacy Program*
- The Department's Plan for Eliminating the Unnecessary Use of SSNs
- The PIA Process
- FISMA Reporting
- What's in the Future
- Questions

Privacy Office

About Us

About the Privacy Office

Senior Agency
Official for Privacy

|

Chief Privacy Officer

|

The Department of
Energy Privacy Office
is Charged with
Overseeing and
Implementing the
Department's Privacy
Program



U.S. DEPARTMENT OF
ENERGY

Office of the Chief
Information Officer

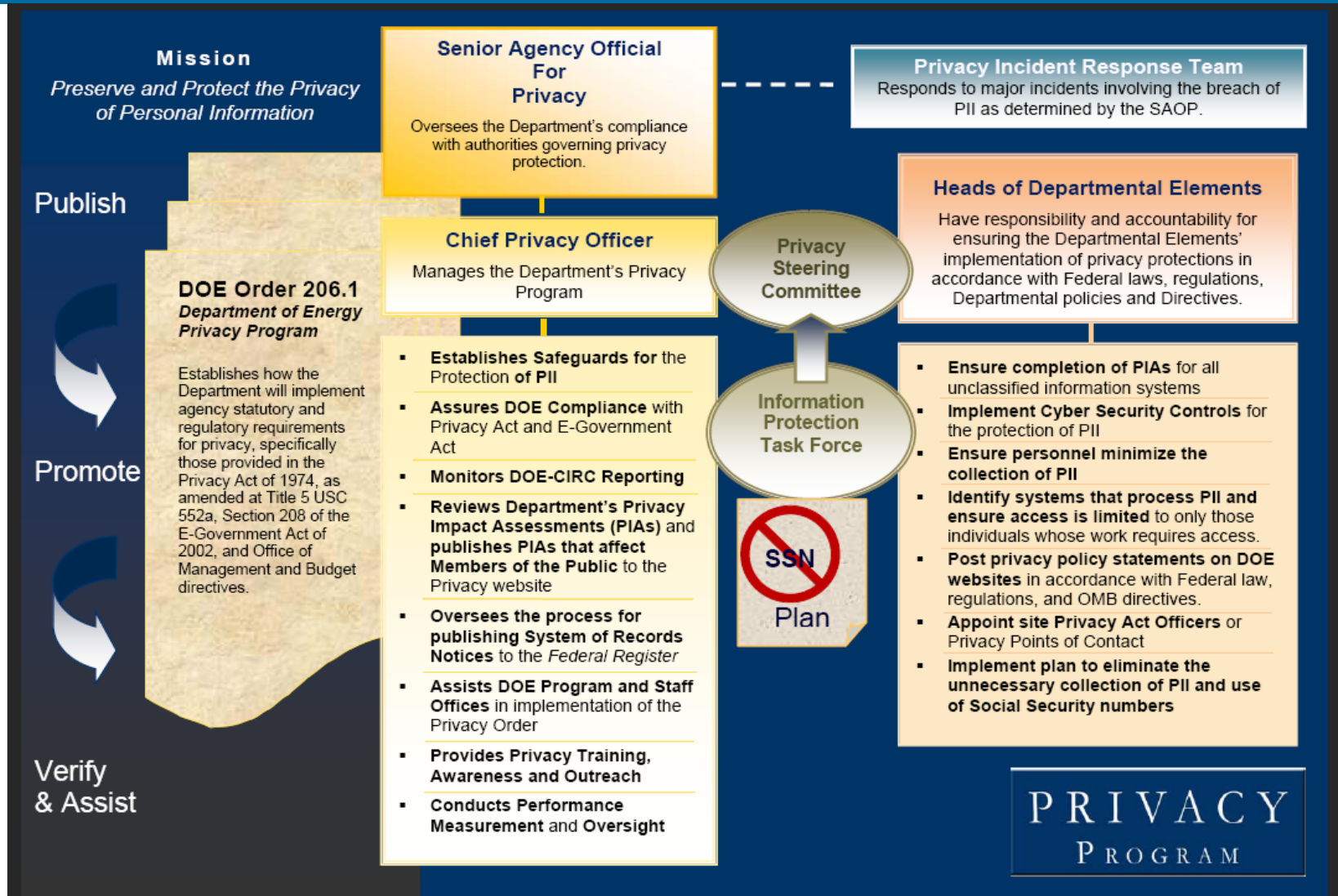
Privacy Office

Objectives

Preserve and Protect the Privacy of
Personal Information

Strengthen Privacy Protections by Building
a Full Lifecycle, Integrated and Auditable
Privacy Program that Preserves the Trust
of the American People

Overview of Department's Privacy Programs



Privacy Office

CPO

- **Establishes Safeguards** for the Protection of PII
- **Assures DOE Compliance** with Privacy Act and E-Government Act
- **Monitors DOE-CIRC Reporting**
- **Reviews Department's Privacy Impact Assessments (PIAs)** and publishes PIAs that affect **Members of the Public** to the Privacy website
- **Oversees the process for publishing System of Records Notices** to the *Federal Register*
- **Assists DOE Program and Staff Offices** in implementation of the Privacy Order
- **Provides Privacy Training, Awareness and Outreach**
- **Conducts Performance Measurement and Oversight**

Privacy Incident
Response Team

Privacy
Steering
Committee

DOE Elements Responsibilities

Privacy Office

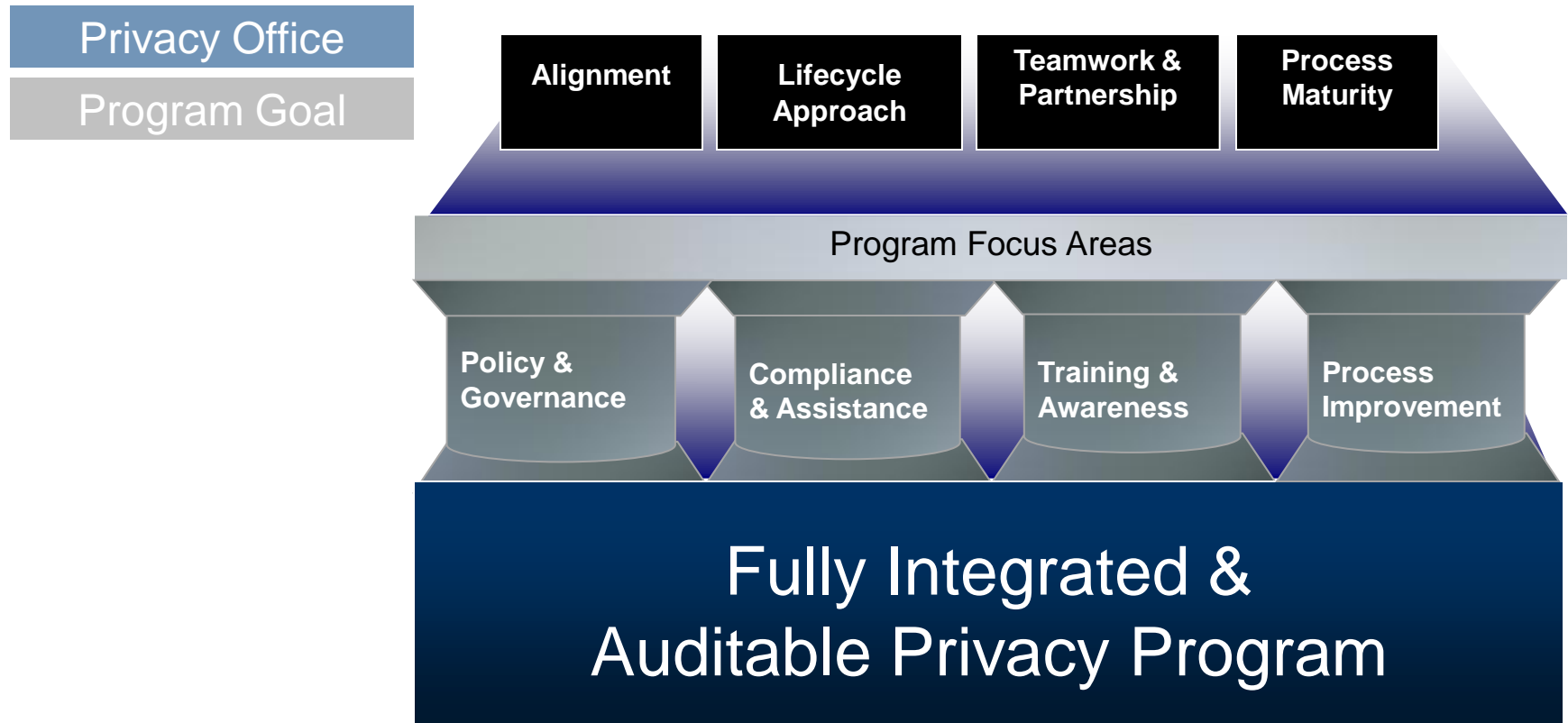
DOE Element

- **Ensure completion of PIAs** for all unclassified information systems
- **Implement Cyber Security Controls** for the protection of PII
- **Ensure personnel minimize the collection of PII**
- **Identify systems that process PII and ensure access is limited** to only those individuals whose work requires access.
- **Post privacy policy statements on DOE websites** in accordance with Federal law, regulations, and OMB directives.
- **Appoint site Privacy Act Officers** or Privacy Points of Contact
- **Implement plan to eliminate the unnecessary collection of PII and use of Social Security numbers**

Privacy Incident
Response Team

Privacy
Steering
Committee

Goal: A Fully Auditable Program



Privacy Office

Partnership

Privacy relies on Good Security.

Security is a Partner.

Policies are complementary.



DOE O206.1, *Department of Energy Privacy Program*

Privacy Office

Privacy Order

U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 206.1

Approved: 1-16-09

SUBJECT: DEPARTMENT OF ENERGY PRIVACY PROGRAM

1. PURPOSE

- a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) directives.
- b. Establish a Departmental training and awareness program for all DOE Federal and contractor employees to ensure personnel are cognizant of their responsibilities for—
 - (1) safeguarding Personally Identifiable Information (PII) and
 - (2) complying with the Privacy Act.
- c. Provide Departmental oversight to ensure compliance with Federal statutes, regulations and Departmental Directives related to privacy.

2. CANCELLATION. DOE N 206.5, *Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information*, dated 10-09-07, is canceled. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Contractor requirement documents (CRDs) that have been incorporated into or attached to a contract remain in effect until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY

- a. DOE Elements. Except for the exclusions in paragraph 3c, this Order applies to all Departmental Elements, including those created after the Order is issued. (Go to www.directives.doe.gov/pdfs/refdocs/org-list.pdf for the current listing of Departmental Elements.)

The Administrator of the National Nuclear Security Administration (NNSA) will ensure that NNSA employees and contractors comply with their respective responsibilities under this Order.

- b. DOE Contractors. Except for the exclusions in paragraph 3c, the CRD (Attachment 1) sets forth contractor requirements. The CRD will apply to the extent set forth in each contract.
- c. Exclusions. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511, and to

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Management

Ensure Implementation of

- Privacy Act
- E-Government Act
- OMB directives

Establish a Departmental Training and Awareness program to ensure DOE personnel are cognizant of their responsibilities for—

1. Safeguarding PII
2. Reporting breaches of PII
3. Complying with the Privacy Act.

Provide Departmental Privacy Guidance & Assistance

DOE Plan for Eliminating the Unnecessary Use of SSNs

Privacy Office

SSN Plan

U.S. DEPARTMENT OF ENERGY

PLAN FOR THE REDUCTION OF AGENCY HOLDINGS
OF PERSONALLY IDENTIFIABLE INFORMATION &
ELIMINATION OF THE UNNECESSARY USE OF
SOCIAL SECURITY NUMBERS



JANUARY 2009
FINAL REPORT

INFORMATION PROTECTION TASK FORCE REPORT
TO THE SENIOR AGENCY OFFICIAL FOR PRIVACY

- Baseline Inventory
- Site Assistance
- Assess Alternatives
- Review Technology Solutions
- Privacy Steering Committee

U.S. DEPARTMENT OF ENERGY

PLAN FOR ELIMINATING THE
UNNECESSARY COLLECTION AND
USE OF SOCIAL SECURITY NUMBERS

DOE is working to protect
privacy by eliminating the
unnecessary collection and use
of Social Security numbers.



CHIEF PRIVACY OFFICER

For more information visit the DOE Privacy homepage at
energy.gov by clicking on the Privacy icon or by email at
privacy@hq.doe.gov.

PRIVACY
PROGRAM



U.S. DEPARTMENT OF
ENERGY


Office of the Chief
Information Officer


Privacy Impact Assessment Process

Privacy Office

New PIA Process

PRIVACY IMPACT ASSESSMENT: **ORG NAME – SYSTEM NAME**
PIA Template Version 3 – May, 2009

 **Department of Energy**
Privacy Impact Assessment (PIA)



Guidance is provided in the template. See DOE Order 206.1, *Department of Energy Privacy Program*, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: <http://www.directives.doe.gov/pdfs/doe/doeetcd/neword/206.1.pdf>

Please complete electronically; no hand-written submissions will be accepted.
This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	Date the assessment was completed.	
Departmental Element & Site	The official list of Departmental Elements can be accessed at www.directives.doe.gov/pdfs/reftools/org-list.pdf . Please also list the site location of the system with as much specificity as possible (e.g. DOE Headquarters, Forrestal, 1G-053 server room).	
Name of Information System or IT Project	Enter the name of the information system. If the system is part of an enclave or general support system (GSS), please include the name of the enclave or GSS along with the name identifying the application or subsystem being assessed.	
Exhibit Project UID	Enter the project unique identifier used for capital planning (eCPIC) or the contract name that provides the funding for the system.	
New PIA <input type="checkbox"/>	Please indicate whether this is a new PIA or an update to an existing PIA. List the name of the PIA being updated.	
Update <input type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
System Owner	System Owners are Departmental Element officials responsible for monitoring the information systems under their purview to ensure compliance with this Order. System Owners are responsible for the overall procurement, development, integration, maintenance, secure operation, and safeguarding of Privacy information including PII for their information system(s). System owners may be Federal or contractor	Use the full phone number and email. For example (202) 556-1212 John.doe@hq.doe.gov

PRIVACY PROGRAM 1

Privacy Needs Assessment

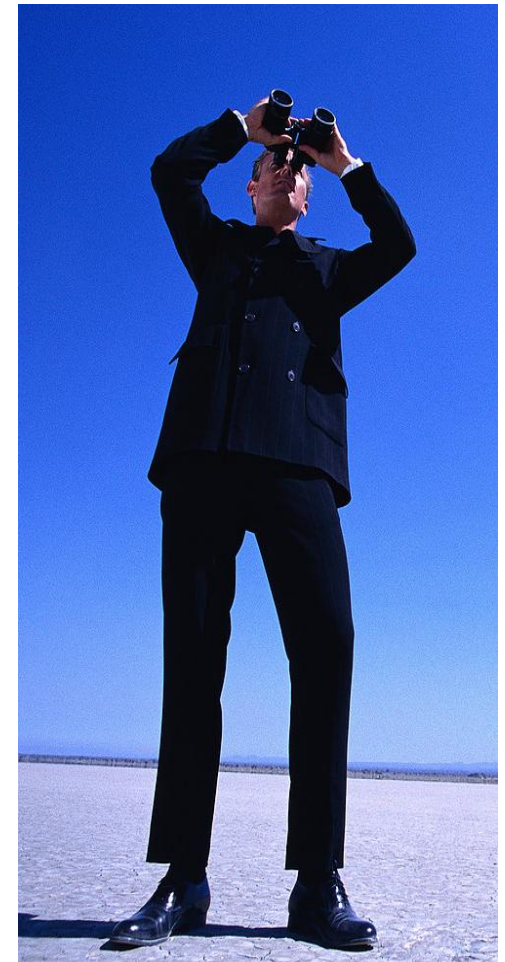
- ✓ 4 Threshold Questions
- ✓ Tiered Approach
- ✓ Expanded Guidance
- ✓ O 206.1, Appendix A

What's In the Future?

Privacy Office

Future

- Increased Risk & Media Attention
- Privacy Advocates Stepping Up the Pressure
- Administration & Congress
- OMB



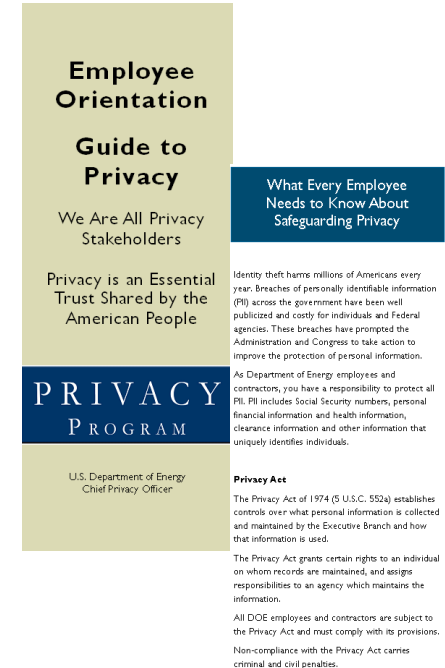
Jerry Hanley
Chief Privacy Officer
U.S. Department of Energy

(202) 586-0483

privacy@hq.doe.gov

DOE Privacy Website:

From energy.gov, click on Privacy Program at the bottom of the DOE homepage.



Employee Orientation

Guide to Privacy

We Are All Privacy Stakeholders

Privacy is an Essential Trust Shared by the American People

PRIVACY PROGRAM

U.S. Department of Energy
Chief Privacy Officer

What Every Employee Needs to Know About Safeguarding Privacy

Identity theft harms millions of Americans every year. Breaches of personally identifiable information (PII) across the government have been well publicized and costly for individuals and Federal agencies. These breaches have prompted the Administration and Congress to take action to improve the protection of personal information.

As Department of Energy employees and contractors, you have a responsibility to protect all PII. PII includes Social Security numbers, personal financial information and health information, clearance information and other information that uniquely identifies individuals.

Privacy Act

The Privacy Act of 1974 (5 U.S.C. 552a) establishes controls over what personal information is collected and maintained by the Executive Branch and how that information is used.

The Privacy Act grants certain rights to an individual on whom records are maintained, and assigns responsibilities to an agency which maintains the information.

All DOE employees and contractors are subject to the Privacy Act and must comply with its provisions. Non-compliance with the Privacy Act carries criminal and civil penalties.

Scenario: An Incident Has Occurred



You are the program manager at one of the Department's field sites. One of your team reports to you that several laptops are missing. This person suspects the laptops may have had personnel information.

What do you do?

How Should You Respond?



- ✓ Report the Breach Immediately
 - ✓ Management
 - ✓ DOE-CIRC/US-CERT
- ✓ Did the Laptop Contain PII? Type?
- ✓ Was the Laptop Encrypted?
- ✓ How Many Affected?
- ✓ Notification?
- ✓ Keep a Log of Everything
- ✓ Follow Up / Corrective Action
- ✓ Order 206.1, Appendix B